

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

DHI GROUP, INC. F/K/A DICE HOLDINGS, §
INC. AND RIGZONE.COM, INC., §

Plaintiffs, §

vs. §

DAVID W. KENT, JR., SINGLE §
INTEGRATED OPERATIONS PORTAL, §
INC. D/B/A OILPRO AND OILPRO.COM, §
ESTEVAN DUFRIN, MATTHEW KENT, §
BRYAN ROBINS, JEREMY ANTONINI, §
AND JOHN DOE NOS. 1-10, §

Defendants. §

C.A. NO.: _____

**PLAINTIFFS DHI GROUP, INC.'S AND RIGZONE.COM, INC.'S
ORIGINAL COMPLAINT**

Plaintiffs DHI Group, Inc. f/k/a Dice Holdings, Inc. (“DHI Group”) and Rigzone.com, Inc. (“Rigzone”) (collectively, “Plaintiffs”) file this Original Complaint against Defendants David W. Kent, Jr. (“David Kent”), Single Integrated Operations Portal, Inc. d/b/a Oilpro and Oilpro.com (“Oilpro”), Estevan Dufrin (“Dufrin”), Matthew Kent, Bryan Robins (“Robins”), Jeremy Antonini (“Antonini”), and John Doe Nos. 1-10 (collectively, “Defendants”).

I. Nature and Summary of Complaint

1. This lawsuit concerns the unlawful theft and misappropriation of proprietary information and arises under and is brought to enforce rights created by the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. §§ 2701, *et seq.*, the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961 *et. seq.*, the Texas Uniform Trade Secrets Act, TEX. CIV. PRAC. & REM. CODE

§§ 134A.001 *et seq.*, the Texas Harmful Access by Computer Act, TEX. CIV. PRAC. & REM. CODE §§ 143.001 *et seq.*, the Texas Theft Liability Act, TEX. CIV. PRAC. & REM. CODE §§ 134.001 *et seq.*, and Texas common law and seeks damages (including exemplary damages) and injunctive relief.

2. David Kent agreed with Dufrin to access information belonging to Rigzone’s website, Rigzone.com, and DHI Group without authorization and to defraud DHI Group, Rigzone’s owner. David Kent accessed a database maintained by Rigzone without authorization and stole member information, including information from over 450,000 unique resumes. David Kent then exploited this information by inviting many of Rigzone’s members to join a new competing website he had created called Oilpro.com. Similarly, Dufrin accessed information in Plaintiffs’ Google Analytics account without authorization and forwarded the information to David Kent. After surreptitiously accessing Rigzone’s computer systems and stealing its valuable database of member resumes, profiles, and other confidential information, David Kent then attempted to defraud DHI Group by (i) misrepresenting that his new website had increased its membership through standard marketing methods, (ii) using misappropriated data to divert Rigzone’s members and customers to do business with Oilpro and therefore directly compete with Rigzone, and (iii) attempting to sell the new website—created by stealing from Rigzone—to DHI Group for tens of millions of dollars. In furtherance of this scheme, David Kent caused emails and telephone calls to be sent to the CEO of DHI Group.

3. These are only some of the steps David Kent and the other Defendants have taken to defraud Plaintiffs and deprive them of the value of their businesses. David Kent also set up at least one secret “backdoor entry” into Rigzone’s computer systems, kept that “backdoor” secret from DHI Group and Rigzone, and had a backup of the entire Rigzone website placed on an

external drive that disappeared near the time of his departure from Rigzone. Taken together, David Kent and the other Defendants have engaged in illegal and tortious conduct to sell Rigzone to DHI Group for over \$51 million and to compete with Plaintiffs.

4. The truth (or at least a significant portion of it), however, has now been uncovered. David Kent is now facing criminal charges in New York federal court for conspiracy and wire fraud. Dufrin was also under investigation and chose to become a cooperating witness with authorities. David Kent, Dufrin, Oilpro, Mathew Kent, Robins, Antonini, and unknown wrongdoers must now answer civilly for their illegal and tortious conduct.

II. Parties

5. Plaintiff DHI Group, Inc. is a Delaware corporation and maintains its principal place of business in New York, New York.

6. Plaintiff Rigzone.com, Inc. is a Texas corporation and maintains its principal place of business in Houston, Texas.

7. Defendant David W. Kent, Jr. is an individual residing in Montgomery County, Texas and may be served with process at 54 N Gary Glen Circle Spring, Texas 77382-2623.

8. Defendant Single Integrated Operations Portal, Inc. d/b/a Oilpro and Oilpro.com is a Texas corporation with its principal place of business in Houston, Harris County, Texas. Oilpro may be served through its registered agent, David W. Kent, Jr., at 110 Vintage Park Blvd., Building J, Suite 245, Houston, Texas 77070.

9. Defendant Estevan Dufrin is an individual residing in Harris County, Texas and may be served with process at 110 Vintage Park Blvd., Building J, Suite 245, Houston, Texas 77070-4047 or 6119 Morningcrest Ct., Spring, Texas 77389-3756.

10. Defendant Matthew Kent is an individual residing in Coryell County, Texas and may be served with process at 110 Vintage Park Blvd., Building J, Suite 245, Houston, Texas 77070-4047 or 11606 Wilcant Lane, Cypress, Texas 77429.

11. Defendant Bryan Robins is an individual residing in Harris County, Texas and may be served with process at 110 Vintage Park Blvd., Building J, Suite 245, Houston, Texas 77070-4047 or 16602 Saddle Ridge Pass, Cypress, Texas 77433-5945.

12. Defendant Jeremy Antonini is an individual residing in Bexar County, Texas and may be served with process at 806 Highland Knoll, San Antonio, Texas 78260-3530.

13. Defendants John Doe Nos. 1-10 are as yet unnamed Oilpro employees, contractors, agents, and/or investors who participated and acted in concert with Oilpro, David Kent, Dufrin, Matthew Kent, Robins, and Antonini in their scheme to unlawfully access and misappropriate Plaintiffs' trade secrets and proprietary information and divert Rigzone's members for Oilpro's benefit. Plaintiffs are unaware of the names and capacities, whether individual, corporate, associate, or otherwise, of the Defendants John Doe Nos. 1-10. Discovery will establish the John Doe Defendants' identities, and the full nature and extent of their involvement in the misconduct, which caused the damages alleged herein.

14. All wrongful conduct detailed in this complaint that was undertaken by David Kent, Dufrin, Matthew Kent, Robins, Antonini, and any John Doe Nos. 1-10 who have been employed by Oilpro was undertaken both in their individual capacities and in their roles as employees, shareholders, directors, managers, and/or officers of Oilpro.

III. Jurisdiction and Venue

A. Jurisdiction

15. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because Plaintiffs' federal claims arise under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the

Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. § 2701 *et. seq.*, and the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961 *et. seq.*

16. This Court has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367, because those claims are so closely related to claims in the action within the Court's original jurisdiction that they form part of the same case or controversy and therefore make the Court's exercise of supplemental jurisdiction appropriate.

17. This Court has both general and specific jurisdiction over Defendants David Kent, Dufrin, Matthew Kent, Robins, and Antonini as (i) David Kent resides in Montgomery County, Texas which lies within the territorial boundary of the Houston Division of the Southern District of Texas, (ii) Dufrin resides in Harris County, Texas which lies within the territorial boundary of the Houston Division of the Southern District of Texas, (iii) Matthew Kent resides in Harris County, Texas which lies within the territorial boundary of the Houston Division of the Southern District of Texas, (iv) Robins resides in Harris County, Texas which lies within the territorial boundary of the Houston Division of the Southern District of Texas, and (v) David Kent, Dufrin, Matthew Kent, Robins, and Antonini's wrongful conduct against Plaintiffs took place in Harris County, Texas. The exercise of personal jurisdiction over David Kent, Dufrin, Matthew Kent, Robins, and Antonini (all of whom reside in Texas) therefore does not offend traditional notions of fair play and substantial justice.

18. This Court has general and/or specific jurisdiction over Oilpro because it maintains its principal place of business in Texas, and because Plaintiffs' causes of action arise from and are directly related to Oilpro's contacts within the Houston Division of the Southern District of Texas. In particular, Oilpro solicited Rigzone's members from Oilpro's office in Harris County,

Texas. Thus, the exercise of personal jurisdiction over Oilpro does not offend traditional notions of fair play and substantial justice.

B. Venue

19. Venue is proper in the United States District Court for the Southern District of Texas, Houston Division, under 28 U.S.C. § 1391(a) because a substantial part of the events or omissions giving rise to Plaintiffs' causes of action occurred in this Division, and because several of the Defendants reside in this Division. Specifically, many of the acts and transactions, including Defendants' theft and/or misappropriation of Plaintiffs' trade secrets and confidential information and Defendants' use of instrumentalities of interstate commerce, took place and/or continue to take place in Harris County, Texas and the Southern District of Texas, Houston Division.

IV. Facts

A. History and Sale of Rigzone

20. In approximately 2000, David Kent launched Oceandril Data Services ("ODS") as a website that listed offshore drilling rigs and other oil and gas equipment and machinery for sale or lease. After receiving complaints about the use of the acronym ODS by another company that was already utilizing that acronym, David Kent changed the website name to Rigzone which, in an effort to gain additional site traffic, branched into new offerings such as aggregating industry news. Rigzone began to offer job postings for professionals working in the oil and gas industry in and near the Houston area and the Gulf Coast region. This service became the key driver to Rigzone's business.

21. In August 2010, DHI Group acquired Rigzone from David Kent and other Rigzone investors for approximately \$51 million. David Kent owned approximately 70% of Rigzone and therefore received over \$35 million by selling Rigzone, its website, and its assets—including its

database of member resumes, profiles, and other confidential information—to DHI Group. Other defendants, including Matthew Kent, Robins, and Antonini, also profited handsomely from the sale of Rigzone to DHI Group. Like David Kent, Matthew Kent, Robins, Antonini, and others stayed with Rigzone for a period of time after the acquisition—only later to join Oilpro and begin competing with Rigzone using the tortious methods complained of herein.

22. DHI Group is a publicly-traded company that operates several websites that help organizations find the best talent and help professionals find the best jobs and advance their careers. DHI Group services a number of different industries, including technology, financial services, and healthcare. DHI Group offers several products, including resume databases and job postings, and allows customers to purchase recruitment packages, job postings, and advertisements.

23. The Rigzone acquisition was part of a number of strategic acquisitions and investments by DHI Group to become a leader in the energy industry. In addition to the over \$51 million acquisition of Rigzone, DHI Group acquired two other companies—World Wide Worker and Oil Careers—to provide a unified, international platform focused exclusively on professionals in the energy industry. DHI Group's investment in the energy industry went beyond these three acquisitions to increase and improve the services offered by Rigzone to its members and its customers, and thereby increase Rigzone's value to the DHI Group.

24. Rigzone offers an on-line platform specific to professionals in the energy industry and has developed marketing and engagement methods to create and present content that energy professionals find valuable. These efforts attract professionals with the specific intent to advance their careers in the energy industry, and it is that focus and attraction that generates value for Rigzone's customers (recruiters and employers in the energy industry worldwide).

25. Rigzone allows its members—oil and gas professionals—to create online profiles that contain personal and professional information. As part of their profiles, members can also upload their resumes, which are assigned unique numerical identifiers (“Resume ID numbers”). The profiles are contained in a database maintained by Rigzone (the “Members Database”). Members are assigned login credentials (*i.e.*, usernames and passwords) when they create their profiles. Members use these login credentials to access their profiles.

26. Rigzone allows members to upload their resumes as part of their user profiles, which can be used to apply for job openings posted by recruiters and employers. Similarly, recruiters and employers who pay for access to Rigzone’s members can also solicit members (depending on an individual member’s privacy settings) directly for job opportunities. Rigzone’s Members Database is a closed environment, meaning that only Rigzone’s paying customers may access it. In other words, unlike other websites such as LinkedIn, the member profiles on Rigzone are not published, or otherwise made available, to the public.

27. Rigzone’s targeted marketing and engagement efforts are designed to continually increase the Members Database by adding new members and to keep existing members engaged by, among other things, updating their profiles and applying to jobs posted on the site. It is therefore not only the size of Rigzone’s Members Database that is valuable, but also its quality and the focus on active energy professionals looking to advance their careers that makes it attractive to recruiters and employers worldwide and unique and valuable trade secrets held by Plaintiffs.

28. Rigzone also derives revenue from selling advertising space on its website. The desirability and pricing of such space is driven, in part, by the number of users who visit the website and the number of page views by users.

29. To protect Rigzone's Members Database, confidential search engine analytics, and other proprietary information, Rigzone invested substantial time and resources throughout the relevant time period developing, purchasing, installing, and providing secure access to its computer systems and member information.

30. Rigzone retains computer professionals to update, remediate, and ensure the safety and security of its electronic data, including its proprietary member information.

31. To further protect its, and its members', confidential data, Rigzone only allows access to its computer systems by its employees or other authorized personnel. This access is password-protected. Upon any employee's departure, Rigzone's procedure is to shut down password access to its computer systems for the departed employee.

32. As explained above, DHI Group has continued to operate, develop, and invest in Rigzone to make it the leading online platform for professionals in the energy industry.

B. Formation of Oilpro

33. On or around October 1, 2013, immediately after the earliest possible expiration of his non-compete period with Rigzone and DHI Group, David Kent publicly announced the launch of Oilpro.com and made the entire website available to the public.

34. David Kent, however, had for some time secretly been laying the foundation to compete with Rigzone and other websites owned by DHI Group. As noted above, DHI Group owns and operates numerous websites, in addition to Rigzone, that service other professional industries, such as technology, financial services, healthcare, and hospitality.

35. In order for the business that David Kent was contemplating to rapidly become competitive, David Kent devised a scheme to steal Plaintiffs' files and confidential and proprietary information after selling Rigzone and direct that information into his newly-formed entity. When David Kent shared with Plaintiffs information about Oilpro's membership figures

and its growth, Plaintiffs were stunned by those figures. The membership growth boasted by David Kent was simply unheard of even to DHI Group which had been operating professional platforms in numerous industries for many years.

36. To further this criminal and civil misconduct, David Kent had secretly installed a complex “backdoor” that would allow him to surreptitiously access Rigzone’s computer systems, including its Members Database, after he sold the company and founded a competitor. Indeed, David Kent installed or directed the installation of an administrative access point to Rigzone’s resume database, which allowed for direct access to the resumes of Rigzone’s members that bypassed the need for account credentials. It allowed a user with knowledge of its existence and functionality to navigate to the standard resume search page on Rigzone and have full viewing access of a given job seeker’s password-protected resume profile without having to login with resume search credentials.

37. The access point was installed in a manner that prevented its detection by Rigzone’s administrative reporting tools and other security measures. Even the forensic experts retained to investigate the criminal security breach emphasized the complexity of David Kent’s “backdoor” and the difficulty in detecting the presence of David Kent’s access point.

38. In order to gain access from the outside, an individual would need specific knowledge of the code, the presence of the vulnerability, the sequential resume identification numbering system, and the knowledge of the key words necessary to utilize the access point. David Kent knew all of this and kept it a secret.

39. Although David Kent was aware of the “backdoor,” he intentionally withheld that information. After selling Rigzone to DHI Group for approximately \$51 million, David Kent continued to work with Rigzone as an employee of DHI Group. During this time, David Kent

did not disclose the existence of the “backdoor.” Instead, David Kent began taking steps to form his competitor website, Oilpro.

40. Immediately after his consulting agreement ended, in January 2012, David Kent formed Single Integrated Operations Portal, Inc. (“SIOPCO”) to act as a parent company for the websites he planned to design to compete with DHI Group, and in November 2012, David Kent registered the Oilpro domain name under SIOPCO’s umbrella.

41. In 2013, as David Kent continued preparing to launch his competing business, he brought the Oilpro website online. He even displayed a countdown ticker on the website for Oilpro’s launch, which was timed to count down to the expiration of his non-compete.

42. For years, David Kent had been plotting against Plaintiffs. For example, he had asked at least one Rigzone employee to prepare a backup copy of Rigzone’s entire website for him, which based on information and belief was never created. Later, however, David Kent asked another Rigzone employee to prepare for him an external drive containing a backup of the entire Rigzone website. On this occasion, the backup drive was created and stored on an external drive. Following David Kent’s departure, it was discovered that this external drive went “missing”.

43. In October 2013—when his countdown ticker hit “zero”—Oilpro’s site became operational and began competing with Rigzone and DHI Group.

44. In or around December 2013, within a month of leaving Rigzone, Dufrin was hired by David Kent to begin working at Oilpro. Dufrin reported to David Kent and remains currently employed by Oilpro.

45. David Kent then began soliciting other Rigzone employees to join him at Oilpro. David Kent targeted and hired employees with whom he had a pre-existing relationship and who were intimately familiar with Rigzone’s Members Database and computer systems.

46. David Kent and Oilpro hired Matthew Kent—David Kent’s brother—to serve as head of corporate sales. Before joining Oilpro, Matthew Kent was employed by Rigzone where he served as the Vice President of Sales (both before and after DHI Group acquired Rigzone). Accordingly, Matthew Kent was experienced with Rigzone’s business, was familiar with Rigzone’s Members Database, and had the most intimate knowledge of Rigzone’s relationships with its largest recruiter and employer customers. Based on his knowledge and experience, Matthew Kent knew that sales to recruiter and employer customers were tied to the size of the platform’s membership and also knew realistic rates of membership growth in the industry. Consequently, Matthew Kent knew that Oilpro’s rapid growth could not have been the result of legitimate marketing efforts or other legitimate business practices. At Oilpro, Matthew Kent worked closely with David Kent and had the experience, skills, position, opportunity, and motive to support, assist, and participate with David Kent, Oilpro, and others in the illegal and tortious conduct towards the Plaintiffs.

47. David Kent and Oilpro hired Robins to serve as head of advertising sales. Before joining Oilpro, Robins was employed by Rigzone where he served as Vice President of Sales (both before and after DHI Group acquired Rigzone). Accordingly, Robins was experienced with Rigzone’s business practices, and also had intimate knowledge of Rigzone’s advertising sales. Based on his knowledge and experience, Robins knew that advertising sales were tied to the size of the platform’s membership and volume of website traffic, and also knew realistic rates of membership growth in the industry. Consequently, Robins knew that Oilpro’s rapid growth could not have been the result of legitimate marketing efforts or other legitimate business practices. At Oilpro, Robins worked closely with David Kent and had the experience, skills,

position, opportunity, and motive to support, assist, and participate with David Kent, Oilpro, and others in the illegal and tortious conduct towards the Plaintiffs.

48. David Kent and Oilpro hired Antonini to serve as chief of technology. Before joining Oilpro, Robins was employed by Rigzone where he served as Vice President of Technology (both before and after DHI Group acquired Rigzone). Accordingly, Antonini was experienced with Rigzone's business practices, computer systems, and Members Database. With David Kent and Antonini on board, Oilpro had the technical skills necessary to infiltrate Plaintiffs' computer systems. In fact, David Kent and Antonini were the persons most familiar with the code for Rigzone.com. At Oilpro, Antonini worked closely with David Kent and had the experience, skills, position, opportunity, and motive to support, assist, and participate with David Kent, Oilpro, and others in the illegal and tortious conduct towards the Plaintiffs.

49. In setting up Oilpro, David Kent sought to reassemble his core team from Rigzone and have the collective group utilize their knowledge and familiarity with Rigzone to quickly ramp up Oilpro's business by misappropriating Plaintiffs' trade secrets and proprietary information. After misappropriating this information, the Defendants then used that information to further Oilpro's business. After the ramp-up, David Kent and the other Defendants intended to sell Oilpro to DHI Group or another purchaser.

50. After joining Oilpro, Dufrin, Matthew Kent, Robins, and Antonini, among others, received an ownership interest in the company.¹ Accordingly, Dufrin, Matthew Kent, Robins, and Antonini stood to financially benefit from Oilpro's growth and success and became financially incentivized to expand Oilpro's member base, whether by diverting Rigzone members or otherwise.

¹ Collectively, Oilpro employees (other than David Kent) own approximately 15% of the company.

51. After assembling his team and commencing what became a long-running practice of unlawfully infiltrating Plaintiffs' computer systems to steal proprietary information and bolster his member base, David Kent began his efforts to market Oilpro for sale to DHI Group.

52. On or about April 24, 2014, David Kent wrote to the CEO of DHI Group and stated: "My original mission was to build something that [DHI Group] would be interested in acquiring. It seemed to work for all parties before."

53. His plan to accomplish this goal was clear: add and convert as many members to Oilpro, by whatever means necessary, as quickly as possible. Indeed, an internal email between Dufrin, Kent, and other Oilpro employees entitled "Operation Resume Hoard - Part 1" plainly discloses their scheme: "Objective: Increase number of searchable resumes in the back end for recruiters and build the [Oilpro database]. Goals/Outcomes: Add 100,000 resumes to the [Oilpro database] and Convert 40,000 new members over the 9 months" ("Operation Resume Hoard").

54. Like other professional networking websites, including Rigzone, the financial success of Oilpro depended in large part on the number of users and resumes in the Oilpro database. The larger the number of users, the more money Oilpro could charge recruiting agencies, employers, and advertisers, and the more Oilpro might be worth to potential investors.

55. By January 2016, the Oilpro database had grown to at least 500,000 members. In communications with the CEO of DHI Group, David Kent attributed the growth of the Oilpro database to emailing invitations to contacts of Oilpro members, traditional marketing methods, and "network effects." But Oilpro in fact populated its network using much more nefarious and illegal methods.

C. Unauthorized Access to Plaintiffs' confidential and proprietary information.

The First Round of Hacks

56. On or about February 6, 2014, David Kent accessed member information from the Rigzone database without authorization.

57. On or about February 26, 2014, an individual who had created a member profile with Rigzone contacted Rigzone's customer support line. This individual stated that she had received an email solicitation from Oilpro to use Oilpro's services even though she had never provided any information in the past to Oilpro.

58. An internal review of Rigzone's computer systems revealed no evidence that any employee of Oilpro had viewed this individual's profile using an authorized account created through Rigzone.

59. To determine if the Members Database was being accessed improperly, employees of DHI Group created two fictitious member accounts and populated them with names and email addresses that were only available through Rigzone's Members Database.

60. On or about April 14, 2014, David Kent caused an unsolicited email solicitation to be sent to a member of Rigzone. Specifically, on or about April 14, 2014, the email accounts associated with the fictitious member accounts each received email communications from an employee at Oilpro. The communications solicited the fictitious members to create profiles on Oilpro. An internal review of Rigzone's systems revealed no records of the Oilpro employee from whom the solicitations were sent having viewed the fictitious member accounts on Rigzone. Further, there was no record that any single user of Rigzone had accessed both of the fictitious member accounts.

61. A review of Rigzone's computer systems showed that, between on or about October 17, 2013 and on or about April 15, 2014, approximately 100,000 suspicious hypertext transport

protocol (“HTTP”) requests were made to Rigzone’s Members Database over the Internet (the “First Round of Hacks”). An HTTP request is a computer code command transmitted to a website over the Internet.

62. The HTTP requests related to the First Round of Hacks contained a computer command that directed the Rigzone Members Database to give the user access to specific resumes (the “Get Resume Command”). The Get Resume Command was crafted to exploit a piece of source code unique to Rigzone known only to the individuals who had participated in creating the Rigzone source code. David Kent was one of those individuals.

63. Based upon the intervals between access times and the volume of resumes accessed, the speed with which the HTTP requests related to the First Round of Hacks were submitted suggests very strongly that they were sent using an automated computer program, rather than using manual submissions.

64. Each of the HTTP Requests related to the First Round of Hacks was submitted to Rigzone using a computer that was associated with an Internet Protocol address (“IP address”). The same IP address, however, was not used to submit all of the HTTP requests. Rather, approximately 23 different IP addresses were involved in submitting the approximately 100,000 HTTP Requests related to the First Round of Hacks.

65. Of the approximately 23 IP addresses relating to the First Round of Hacks, approximately 22 were registered to UK Dedicated Servers Limited (“UK DSL”), a company based in the United Kingdom that provides services to obscure a user’s true originating IP address (the “Masked IP Addresses”).

66. An email address associated with David Kent was used to register and pay for an account with UK DSL. Around the time of the First Round of Hacks, David Kent received emails from UK DSL regarding his username and password.

67. Among the IP addresses relating to the First Round of Hacks, at least one IP address was not registered to UK DSL. Instead, this IP Address was registered to SIOPCO, the Internet-based business that was co-founded by David Kent in 2012. Thus, all of the HTTP Requests related to the First Round of Hacks were submitted from IP addresses associated with David Kent.

68. On or about February 6, 2014, February 7, 2014, April 3, 2014, and April 15, 2014, certain of the Masked IP Addresses were used to log into a social media website account registered to David Kent. On those same days, the Masked IP Addresses were also used to submit unauthorized HTTP Requests to Rigzone.

69. In total, the First Round of Hacks involved the unauthorized access of information from approximately 98,000 resumes belonging to members of Rigzone.

70. Following the First Round of Hacks, web traffic to Oilpro increased dramatically, and appears to correlate with the severity of the intrusions into the Rigzone Members Database. Additionally, thousands of Rigzone members whose information was stolen during the First Round of Hacks created profiles on Oilpro, and these profiles created further opportunities for Oilpro to acquire data and value that it would not otherwise would have had access to.

71. After the First Round of Hacks, approximately 796,000 accounts in the Rigzone Members Database were accessed without authorization (the "Hacked Rigzone Accounts"). The Hacked Rigzone Accounts contained approximately 586,560 unique email addresses (the "Hacked Rigzone Email Addresses"). As of January 2016, approximately 17.7 percent of the

Hacked Rigzone Email Addresses had received email invitations to join Oilpro after the Rigzone accounts were accessed without authorization. Approximately 35.7 percent of the Hacked Rigzone Email Addresses who received email invitations eventually joined Oilpro. In total, over 111,000 of the Hacked Rigzone Accounts joined Oilpro after their information on Rigzone was accessed without authorization.

72. Between on or about April 4, 2014 and on or about April 6, 2014, approximately 13,000 accounts in the Rigzone Members Database were accessed (the “April Hacked Rigzone Accounts”). On or about April 14, 2014, almost all of the April Hacked Rigzone Accounts received email invitations to join Oilpro.

73. Then, on approximately April 24, 2014—shortly after the completion of the First Round of Hacks—David Kent contacted the CEO of DHI Group via email. David Kent stated that Oilpro had received an unsolicited offer for investment. David Kent also stated that his original mission with Oilpro was to build something that DHI Group would be interested in acquiring.

74. At that time, DHI Group did not make any offer to invest in or acquire Oilpro from David Kent. In response, David Kent undertook additional hacks against Plaintiffs to boost Oilpro’s membership roster.

The Google Analytics Hacks

75. Google Analytics is a service used by websites to collect data on a variety of statistics relating to user engagement, including (1) number of visits to the website, (2) number of new users, (3) pages viewed per visit, and (4) average duration of each visit. Every Google Analytics account is password-protected, including the Google Analytics accounts associated with Plaintiffs.

76. On or about January 20, 2015, Dufrin accessed information from a Google Analytics account owned by Plaintiffs without authorization. Dufrin then emailed the information to David

Kent. Specifically, on or about January 20, 2015, David Kent contacted Dufrin via email and provided a link to Google Analytics data relating to Oilpro. David Kent wrote to Dufrin: “How do this compare to our friends site” Dufrin replied to David Kent via email and provided a link to data relating to a different website (the “January 2015 Data”).

77. The January 2015 Data came from a password-protected Google Analytics account associated with Plaintiffs, and Dufrin did not have authority to access any password-protected Google Analytics account associated with Rigzone or DHI Group any time after Dufrin left DHI Group on or about November 27, 2013.

78. On or about January 21, 2015, David Kent responded to Dufrin:

Very interesting.... Can we identify the paths on the website that are leading to high [page views]/Session for them? Then we can look at our own and identify our deficiency.

Dufrin replied to David Kent via email:

Yeah sort of. Their page path's are a bit harder to follow due to the various links, but we can determine the landing pages, second pages etc. and come to an educated guess. FYI we hit 345,000 [page views] yesterday, they got 409k. Pretty close.

79. Rigzone had approximately 409,000 page views on January 20, 2015. Thus, David Kent asked Dufrin to determine which pages on Rigzone's website receive high web traffic. Dufrin then responded that it is possible to make an “educated guess” about which pages on Rigzone's website are popular. Dufrin then provided nonpublic information about the number of page views on January 20, 2015 for Rigzone and Oilpro.

80. On or about June 10, 2015, Dufrin contacted David Kent via email and provided two links to data relating to a website (the “June 2015 Data”). Dufrin wrote to David Kent: “*So, I'm trying to scratch the engagement on Rusty² a bit and noticed that the folks searching their jobs*

² On or about December 8, 2014, David Kent wrote an email to several employees of Oilpro and stated: “Rusty = [Rigzone]. Much easier to say and conveys [Oilpro] is the new, non-rusty solution to all of your oil & gas

are 75% return users regardless of the source.” David Kent replied to Dufrin via email and stated: “So ... we don’t have enough jobs ... and our job search sucks. *Solution 1. Get Hannah scraping full-time until we have equal if not more jobs posted per day than Rusty.*” Later that day, David Kent contacted Dufrin via email and stated: “*Why don’t we just hire someone to post all the Rusty jobs? Brute force?*” Therefore, in this exchange, Dufrin and David Kent analyze Rigzone’s users and user profiles and discuss solving Oilpro’s lack of job postings by (i) having Hannah “scrape” others to catch up to Rigzone’s postings and (ii) hiring someone to forcibly acquire all of Rigzone’s job postings.

81. The June 2015 Data came from a password-protected Google Analytics account associated with Plaintiffs, and Dufrin did not have authority to access any password-protected Google Analytics account associated with Plaintiffs any time after Dufrin left DHI Group on or about November 27, 2013.

The Second Round of Hacks

82. Kent, Dufrin, and others continued their efforts to carry out Operation Resume Hoard. Central to this operation was yet another scheme to deprive Plaintiffs of their trade secrets, proprietary data, and market advantages and divert members to Oilpro.

83. Around June 11, 2015, David Kent contacted Dufrin with a link to the resume of an individual claiming to be a “*freelancer for web scraping / crawling / automated data extraction solutions.*” David Kent stated to Dufrin: “*We should hire him and ask him if he can scrape job boards including resume databases*” because “[h]e might find backdoors, etc.” Dufrin responded to David Kent: “*Might be worth a conversation at the least. But yea, if he can find a*

data needs. Also protects my feelings because at one point, that was a product I loved ... it has just gotten a bit rusty.”

backdoor to full CVs ... boom.” “Web scraping” and “crawling” refer to automated programs that extract large amounts of data from websites.

84. On or about July 20, 2015, a DHI Group employee who began—but did not complete—the process of creating a member profile with Rigzone reported receiving an email solicitation from Oilpro. Because the profile was incomplete, this individual’s information was never published in the Rigzone Members Database.

85. A review of Rigzone’s computer systems showed that, between on or about June 17, 2015 and on or about August 2, 2015, approximately 750,000 suspicious HTTP requests were made to the Rigzone Members Database over the Internet (the “Second Round of Hacks”).

86. Each of the HTTP Requests related to the Second Round of Hacks was submitted to Rigzone using a computer that was associated with an IP address. The same IP address, however, was not used to submit all of the HTTP requests. Rather, 10 IP addresses, different than the 23 involved in the First Round of Hacks, were involved in submitting the approximately 750,000 HTTP requests related to the Second Round of Hacks. 660,323 HTTP requests (more than 88% of the total) were submitted by IP addresses in the range 104.128.21.XXX (where XXX is a number between 0 and 255), which is being counted as one unique IP address.

87. Of the 10 different IP addresses relating to the Second Round of Hacks, at least two of them were registered to UK DSL.

88. At least one of the IP addresses relating to the Second Round of Hacks was registered to SIOPCO. An IP address registered to SIOPCO was also used in the First Round of Hacks.

89. Unlike the First Round of Hacks, the Second Round of Hacks exploited a file on Rigzone’s computer system called `resume_writer.asp` (a “.asp” page file is script that generates web page content). Only a person with intimate knowledge of how `resume_writer.asp` works and

how Rigzone catalogued each resume in the Rigzone Members Database would be able to submit the appropriate commands to extract such a large quantity of resumes in such a short period of time.

90. Based upon the intervals between access times and the volume of resumes accessed, the speed with which the HTTP requests related to the Second Round of Hacks were submitted very strongly indicates that they were sent using an automated computer program, rather than using manual submissions.

91. In total, the Second Round of Hacks involved the unauthorized access of information from approximately 700,000 resumes belonging to members of Rigzone. This unauthorized access was pivotal to the success of Operation Resume Hoard.

92. On or about October 25, 2015—shortly after the completion of the Second Round of Hacks—David Kent again contacted the CEO of DHI Group via email. In follow-up to their April 2014 exchange, David Kent stated that Oilpro had taken on an investor the previous year. David Kent further stated that there were few better fits for the software platform of Oilpro than Rigzone. Thus, David Kent was again seeking to create a scenario in which DHI Group would buy Oilpro.

93. DHI Group, however, did not bite at David Kent's overture. In response, Defendants continued Operation Resume Hoard and their hacking strategy.

David Kent's Sales Pitch to DHI Group and the Attempted Third Hack

94. On or about October 28, 2015, David Kent contacted the CEO of DHI Group via email. Relating to the membership of Oilpro, David Kent stated: "Our membership has grown to 540,000 members I believed the Linkedin style growth hacks we applied to [Oilpro] can work in any other market as well. These so-called growth hacks require a social network to be effective." Upon information and belief, "Linkedin style growth hacks" refer to asking Oilpro

members to upload their contacts from LinkedIn.com (“LinkedIn”), another professional networking website, into the Oilpro database. All of these contacts from LinkedIn are then invited to join Oilpro, and the process repeats itself. David Kent did not mention the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, or the Second Round of Hacks in this communication.

95. Approximately one week later, David Kent again contacted the CEO of DHI Group via email. In response to questions from the CEO of DHI Group regarding the growth of Oilpro’s membership, David Kent stated: “We have consistently generated between 20,000 and 50,000 new members per month. The buildup is lumpy just depending on the marketing strategy in place during a given month ... For the first three months, our contacts downloaded LinkedIn contacts for invites to [Oilpro]. This sparked the membership growth and the network effect. I don’t think our growth was dependent on our existing relationships.... With the contacts that [DHI Group] has, we could grow faster than [Oilpro]. We did not do anything unique to [Oil & Gas] to achieve our growth. We have a half dozen strategies that work well and are repeatable.” David Kent thus reiterated the (false) claim that Oilpro’s primary marketing strategy was inviting Oilpro members to upload their contacts from LinkedIn and denied that the growth of Oilpro could be attributable to existing relationships in the oil and gas industry. David Kent further stated that Oilpro used marketing strategies that are repeatable in other industries. Again, David Kent never mentioned the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, or the Second Round of Hacks.

96. On or about November 11, 2015, David Kent e-mailed the CEO of DHI Group. In response to a question regarding the growth of Oilpro’s membership and marketing approaches used, David Kent stated: “From a membership development front, we have several marketing

tactics. LinkedIn is one of them but we also use traditional marketing methods such as Indeed³ (if you can call Indeed traditional). Of late, we have pulled back on ad spend which caused the lumpiness.” Thus, David Kent repeated that one of Oilpro’s marketing strategies was inviting Oilpro members to upload their contacts from LinkedIn, but again did not mention the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, or the Second Round of Hacks.

97. On or about November 25, 2015, David Kent e-mailed the CEO of DHI Group. In response to a question regarding a valuation expectation for an acquisition of Oilpro, David Kent replied: “Last year, we took on [an energy venture capital firm] as an investor. They invested \$3MM at a \$20MM valuation.” Thus, David Kent told DHI Group that Oilpro was valued at \$20 million in 2014. As a result, David Kent implied that DHI Group would need to offer at least \$20 million to purchase Oilpro.

98. On or about December 8, 2015, the CEO, CFO, and General Counsel for DHI Group had a conference call with David Kent to further discuss David Kent’s proposal to sell Oilpro to DHI Group. During the conference call, David Kent stated that the “number one” strategy for growing the membership of Oilpro was asking recruiters and other contacts to upload their LinkedIn contacts to Oilpro and that Oilpro then invited these contacts to join Oilpro. David Kent also attributed the growth of Oilpro to “effort” and the fact that oil and gas is a “safe haven industry.” At the end of the conference call, the CEO of DHI Group expressed interest in scheduling a follow-up conversation to further discuss the practical details of a potential merger or acquisition. David Kent responded that he would “prefer” to have a transaction with DHI Group rather than any other potential investor. David Kent did not mention the First Round of

³ Indeed.com is a website where job-seekers and employers can search for and post resumes and job opportunities.

Hacks, the Google Analytics Hacks, Operation Resume Hoard, or the Second Round of Hacks during the conference call.

99. A review of Rigzone's computer systems showed that, on or about December 11, 2015, at least five suspicious HTTP requests were made to access Rigzone's Members Database over the Internet (the "Attempted Third Hack"). Like the Second Hack, the HTTP requests were made to Rigzone's Members Database using the resume_writer.asp file. The Attempted Third Hack sought to extract the next Resume ID Number in the Members Database following the last resume that had already been extracted during the Second Round of Hacks. Because the resume_writer.asp file had been modified after the Second Round of Hacks, however, the Attempted Third Hack did not result in the extraction of any real resumes from the Members Database.

100. At least one of the IP addresses used to access the Members Database during the Attempted Third Hack was registered to UK DSL. At the time of the Attempted Third Hack, this IP Address was assigned to the UK DSL account associated with David Kent. At the time of the Attempted Third Hack, the UK DSL account associated with David Kent was accessed by an IP Address that was assigned to SIOPCO. Thus, on or about December 11, 2015, David Kent attempted to access member information from the database of a website owned by Plaintiffs without authorization.

101. On or about December 13, 2015—two days after the Attempted Third Hack—the UK DSL account associated with David Kent was accessed by an IP address that was assigned to David Kent's home in Spring, Texas.

102. On or about January 20, 2016, David Kent traveled to New York City for a meeting to discuss a potential acquisition of Oilpro by DHI Group (the "January Meeting"). In describing

the dramatic growth of Oilpro, David Kent stated that the “main mission” for Oilpro employees at the outset was calling friends and asking them to upload their contacts from LinkedIn. Oilpro would then send emails to these LinkedIn contacts, invite them to join Oilpro, and then invite them to upload their contacts from LinkedIn. David Kent stated that this “network effects” strategy was the “core way” and “enough” to grow Oilpro to over 500,000 members in a short period of time. David Kent later stated that Oilpro had the “ability” to increase its membership growth in any given month by putting “effort” into rolling out new features for Oilpro. David Kent did not mention the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, the Second Round of Hacks, or the Attempted Third Hack during the January Meeting.

D. Effect of Hacks on Oilpro Membership

103. On or about January 27, 2016, David Kent emailed a spreadsheet to the CEO of DHI Group with figures and charts describing the growth in membership and number of resumes in the Oilpro members database (the “Spreadsheet”).

104. According to the Spreadsheet, Oilpro gained approximately 3,085 new members in December 2013 and approximately 4,486 new members in January 2014. Oilpro then gained approximately 12,131 new members in February 2014. As mentioned above, a Rigzone member reported receiving an email solicitation to join Oilpro on or about February 26, 2014.

105. Oilpro gained approximately 28,763 new members in April 2014. As mentioned above, the fictitious member accounts in Rigzone received email solicitations to join Oilpro on or about April 14, 2014.

106. Oilpro gained approximately 45,936 new members in June 2014, which was shortly after the First Round of Hacks was completed. David Kent attributes the membership growth in June 2014 to a “Recruiter Directory” and “‘Most Jobs’ + Indeed Campaign.”

107. Oilpro gained approximately 45,823 new members in September 2015, which was shortly after the Second Round of Hacks was completed. David Kent attributes the membership growth in September 2015 to a “Linkedin Campaign.”

108. David Kent did not mention the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, the Second Round of Hacks, or the Attempted Third Hack in the Spreadsheet.

E. The Racketeering Enterprise

109. David Kent and Dufrin engaged in a pattern of predicate racketeering acts referred to here as the Oilpro Enterprise.

110. David Kent and Dufrin participated in a scheme of unlawfully hacking into and infiltrating Rigzone’s private and proprietary computer information—both on Rigzone servers and through Plaintiffs’ Google Analytics accounts—to pilfer Rigzone’s Members Database and Plaintiffs’ online search traffic strategies. David Kent and Dufrin’s scheme was designed to increase Oilpro’s member base in order to enhance Oilpro’s revenue and valuations and then to fraudulently convey legitimate business growth to DHI Group, with the goal of causing DHI Group to purchase Oilpro at an inflated price.

111. This scheme was hatched as early as April 24, 2014, when David Kent wrote to the CEO of DHI Group, stating that he intended “to build something that [DHI Group] would be interested in acquiring. It seemed to work for all parties before.” And this is precisely the path that David Kent and Dufrin pursued, attempting to persuade DHI Group to purchase Oilpro and representing Oilpro’s value at approximately \$20 million based on growth that was attributed, in part, to “network effects” rather than outright theft.

112. In reality, David Kent and Dufrin grew Oilpro by repeatedly and unlawfully hacking into and stealing trade secrets and proprietary information from Plaintiffs. Indeed, David Kent and

Dufrin engaged in more than 850,000 instances of wire communications and infiltrations in order to further their scheme to misappropriate Plaintiffs' information and defraud DHI Group.

113. The benefits to the Oilpro Enterprise and to David Kent and Dufrin took a variety of forms, including an increased member base, increased profits and revenues, furthering the development of Oilpro as a business without the time and costs associated with legitimate marketing efforts, and a tremendous reduction in the competitive advantages of Oilpro's number one competitor, Rigzone. David Kent and Dufrin intended to obtain these benefits when repeatedly engaging in predicate acts to misappropriate trade secrets from Plaintiffs.

114. David Kent and Dufrin also utilized the wires to further their scheme to defraud through each of the HTTP requests in the hacks and attempted hacks, through the Google Analytics Hack, and through various communications with Rigzone and DHI Group in which David Kent emailed figures and charts describing the growth in membership and number of resumes in the Oilpro members database, fraudulently concealing all three hacks (and the attempted final hack in December 2015) as being the bases for this growth. These communications constitute federal wire fraud in violation of 18 U.S.C. § 1834. Further, every other time David Kent and Dufrin transmitted an interstate communication by phone, fax, or e-mail in furtherance of the fraudulent scheme, the participants in the scheme committed federal wire fraud in violation of 18 U.S.C. § 1834. Each such communication was a transmission by a defendant of writings or sounds by wire made for the purpose of executing the scheme to defraud devised by David Kent and Dufrin.

115. David Kent and Dufrin's scheme to defraud Rigzone and DHI Group resulted in damages far exceeding \$5,000. And David Kent and Dufrin received benefits through their scheme to

defraud having a value of more than \$5,000, after Plaintiffs' assets had been wrongfully taken, and knowing that they had been wrongfully taken.

116. The pattern of racketeering acts spanned more than two years. In addition, that pattern of activity posed a threat of continued illicit and illegal activity because it would have continued indefinitely had it not fortuitously been ended by when Plaintiffs discovered that David Kent and Dufrin were unlawfully appropriating information from Plaintiffs' private servers. The acts were related to each other because they all involved the same victims and were designed to bolster Oilpro's member base and business at Plaintiffs' expense, to improve Oilpro's revenues, and to defraud DHI Group (or someone else) into the eventual purchase of Oilpro; and they all involved the same or similar methods of committing crimes against Rigzone and DHI Group, namely, acting through David Kent and Dufrin to unlawfully acquire Plaintiffs' proprietary information.

F. Criminal complaint filed against David Kent

117. On March 23, 2016, Special Agent Evelina Aslanyan with the Federal Bureau of Investigation filed a Complaint against David Kent for violation of 18 U.S.C. §§ 371, 1343, and 2. The Complaint charges David Kent with (i) conspiracy to commit violations of 18 U.S.C. §§ 1030(a)(2)(C), 1030 (c)(2)(B) and 1343 and (ii) wire fraud in violation of 18 U.S.C. §§ 1343 and 2. On June 3, 2016, the U.S. Attorney's Office of the Southern District of New York filed a two-count information against David Kent for (i) conspiracy and (ii) wire fraud. On the same day, David Kent waived indictment of these charges.

V. Claims for Relief

**COUNT I – VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (18 U.S.C.
§§ 1030(A)(2)(C) & (G))
(Against Defendants David Kent, Dufrin, and Oilpro)**

118. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

119. On numerous occasions, including but not limited to during the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, and the Second Round of Hacks, David Kent, Dufrin, and Oilpro violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), by intentionally accessing a protected computer used for interstate commerce or communication, without authorization or exceeding authorized access, and thereby obtaining information from the protected computer and causing loss to one or more persons during a 1-year period aggregating at least \$5,000 in value.

120. Plaintiffs' computer systems that David Kent, Dufrin, and Oilpro accessed on numerous occasions, were used to conduct business nationwide and therefore were "used in or affecting interstate or foreign commerce or communication" and meet the definition of a "protected computer" set forth in 18 U.S.C. § 1030(e)(2)(B).

121. Plaintiffs use intricate privacy and security safeguards to insure that the information on their computer systems are restricted to authorized individuals acting within the scope of their authority.

122. David Kent, Dufrin, and Oilpro were not authorized to access or use Plaintiffs' computer systems on these occasions.

123. On numerous occasions, including but not limited to during the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, and the Second Round of Hacks, David Kent, Dufrin, and Oilpro accessed and transferred Plaintiffs' confidential information for their own use without authorization from Plaintiffs. Thus, David Kent, Dufrin, and Oilpro "obtained information" by accessing Plaintiffs' protected computer.

124. Misappropriating Plaintiffs' confidential information and maintaining such information, David Kent, Dufrin, and Oilpro violated and continue to violate the Computer Fraud and Abuse Act.

125. David Kent, Dufrin, and Oilpro's unauthorized access and use of Plaintiffs' computer systems and misappropriation of confidential information has required Plaintiffs to incur significant costs in (a) assessing the potential damage to Plaintiffs that have been caused by such unauthorized access, use, and misappropriation, (b) responding to the loss of trade secrets and confidential information caused by Defendants' actions, and (c) mitigating the loss of goodwill among Rigzone's members that has resulted from such unauthorized use, access and misappropriation.

126. Plaintiffs have suffered losses and damages by reason of these violations in excess of \$5,000 in the 1-year period from the date the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, and the Second Round of Hacks each commenced.

**COUNT II – VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT
(18 U.S.C. §§ 1030(A)(4) & (G))
(Against Defendants David Kent, Dufrin, and Oilpro)**

127. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

128. On numerous occasions, including but not limited to during the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, and the Second Round of Hacks, David Kent, Dufrin, and Oilpro violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4), by knowingly and with intent to defraud accessing a protected computer without authorization or exceeding authorized access, and by means of such access furthered an intended fraud and obtained something of value worth more than \$5,000. In doing so, David Kent, Dufrin, and

Oilpro also caused loss to one or more persons during a 1-year period aggregating at least \$5,000 in value.

129. Plaintiffs' computer systems that David Kent and Oilpro accessed were used to conduct business nationwide and therefore were "used in or affecting interstate or foreign commerce or communication" and meet the definition of a "protected computer" set forth in 18 U.S.C. § 1030(e)(2)(B).

130. Plaintiffs use intricate privacy and security safeguards to insure that the information on their computer systems are restricted to authorized individuals acting within the scope of their authority.

131. David Kent, Dufrin, and Oilpro were not authorized to access or use Plaintiffs' computer systems on these occasions.

132. David Kent, Dufrin, and Oilpro accessed Plaintiffs' computer systems and obtained and transferred Plaintiffs' valuable confidential information for their own use without authorization from Plaintiffs.

133. David Kent, Dufrin, and Oilpro obtained this valuable confidential information knowingly and with intent to enhance Oilpro's business and revenue and to defraud DHI Group into acquiring Oilpro.

134. By misappropriating Plaintiffs' confidential information and maintaining such information, David Kent, Dufrin, and Oilpro violated and continue to violate the Computer Fraud and Abuse Act.

135. Plaintiffs' confidential data is worth well over \$5,000.

136. Plaintiffs have suffered losses and damages by reason of these violations in excess of \$5,000 in the 1-year period from the date the First Round of Hacks, the Google Analytic Hacks, Operation Resume Hoard, and the Second Round of Hacks each commenced.

**COUNT III – VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (18 U.S.C.
§§ 1030(A)(5)(A) & (G))
(Against Defendants David Kent, Dufrin, and Oilpro)**

137. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

138. On numerous occasions, including but not limited to during the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, and the Second Round of Hacks, David Kent, Dufrin, and Oilpro violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(C), by knowingly causing transmission of information and, as a result, intentionally causing damage without authorization to a protected computer and causing loss to one or more persons during a 1-year period aggregating at least \$5,000 in value.

139. Specifically, on numerous occasions, including but not limited to during the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, and the Second Round of Hacks, David Kent, Dufrin, and Oilpro knowingly caused the transmission of information by downloading data from Plaintiffs' computer systems to an outside location. David Kent, Dufrin, and Oilpro additionally caused the transmission of information by subsequently transmitting that data to others.

140. David Kent, Dufrin, and Oilpro's downloading the data from Plaintiffs' secure computer systems to an outside location rendered Plaintiffs' computer systems and data less secure, causing Plaintiffs damage.

141. David Kent, Dufrin, and Oilpro were not authorized to cause the transmission of the data from Plaintiffs' computer systems to a different location on these occasions.

142. Plaintiffs' computer systems that David Kent and Oilpro accessed on these occasions were used to conduct business nationwide and therefore were "used in or affecting interstate or foreign commerce or communication" and meet the definition of a "protected computer" set forth in 18 U.S.C. § 1030(e)(2)(B).

143. Plaintiffs have suffered losses and damages by reason of these violations in excess of \$5,000 in the 1-year period from the date the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, and the Second Round of Hacks each commenced.

**COUNT IV – VIOLATION OF THE STORED WIRE AND ELECTRONIC COMMUNICATIONS AND
TRANSACTIONAL RECORDS ACCESS ACT (18 U.S.C. §§ 2701(A)(1) & 2707)
(Against Defendants David Kent, Dufrin, and Oilpro)**

144. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

145. On numerous occasions, including but not limited to during the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, and the Second Round of Hacks, David Kent, Dufrin, and Oilpro violated the Stored Communications Act, 18 U.S.C. § 2701(a)(1), by knowingly and intentionally accessing, without authorization, a facility through which an electronic communication service is provided and thereby obtained, altered, or prevented authorized access to a wire or electronic communication while it was in electronic storage.

146. Specifically, on numerous occasions, including but not limited to during the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, and the Second Round of Hacks, David Kent, Dufrin, and Oilpro violated the Stored Communications Act, 18 U.S.C. §§ 2701 *et. seq.*, by accessing Plaintiffs' computer systems, accessing numerous Rigzone member accounts, and obtaining information, resumes, and other electronic communications prepared by Rigzone members while that information was in electronic storage.

147. Rigzone.com is a website that allows its members to send or receive electronic communications and that meets the definition of an “electronic communication service” set forth in 18 U.S.C. § 2711(1) (adopting definitions from 18 U.S.C. § 2510) and 18 U.S.C. § 2510(15) (definition of “electronic communication service”). Thus, Plaintiffs’ computer systems are facilities through which an electronic communication service is provided.

148. Plaintiffs’ intricate privacy and security safeguards to insure that the information on its computer systems and the facility through which Plaintiffs’ electronic communication service is provided is restricted to authorized individuals acting within the scope of their authority.

149. David Kent, Dufrin, and Oilpro were not authorized to access or use Plaintiffs’ computer systems and the facility through which Plaintiffs’ electronic communication service is provided on these occasions.

150. David Kent, Dufrin, and Oilpro knowingly, willfully, and intentionally accessed Plaintiffs’ computer systems and the facility through which Plaintiffs’ electronic communication service is provided.

151. Plaintiffs are “person[s] aggrieved” by David Kent, Dufrin, and Oilpro’s violation of the Stored Communications Act, 18 U.S.C. §§ 2701 *et. seq.*, as they are persons against whom the interception was directed. *See* 18 U.S.C. § 2707(a); 18 U.S.C. § 2711(1) (adopting definitions from 18 U.S.C. § 2510); 18 U.S.C. § 2510(11) (definition of “aggrieved person”).

152. Plaintiffs have suffered damages as a result of David Kent, Dufrin, and Oilpro’s violation of the Stored Communications Act and are entitled to recover their actual damages and revenues and/or gains made by David Kent, Dufrin, and Oilpro as a result of the violation. 18 U.S.C. § 2707(c).

153. Pursuant to 18 U.S.C. § 2707(c), Plaintiffs are also entitled to recover exemplary damages for David Kent, Dufrin, and Oilpro's willful or intentional violation of the Stored Communications Act, as described above.

154. Pursuant to 18 U.S.C. § 2707(c), Plaintiffs are also entitled to recover their court costs and reasonable and necessary attorneys' fees for David Kent, Dufrin, and Oilpro's violation of the Stored Communications Act, as described above.

**COUNT V – VIOLATION OF RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT (18 U.S.C. §1962(A))—INVESTMENT OF INCOME FROM RACKETEERING ACTIVITY
(Against Defendants David Kent and Dufrin)**

155. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

156. David Kent and Dufrin invested the proceeds of racketeering activity in the Oilpro Enterprise in violation of 18 U.S.C. § 1962(a).

157. Some of the proceeds from the racketeering acts of David Kent and Dufrin, including increased revenues and profits resulting from members who were unlawfully stolen from Rigzone's Members Database (and new members gained through members gained or who joined through members whose information was misappropriated from Plaintiffs' computer systems) and from members obtained from David Kent and Dufrin's unlawful access to and implementation of search strategies obtained through the Google Analytics Hacks, were then invested into the Oilpro Enterprise by Defendants.

158. As a result, Plaintiffs were injured in their business and property.

159. Plaintiffs request that this Court enter judgment that David Kent and Dufrin have violated 18 U.S.C. § 1962(a). Plaintiffs are entitled to damages incurred as a result of David Kent and Dufrin's prohibited conduct, trebled by statute, plus reasonable attorneys' fees and costs of suit.

**COUNT VI – VIOLATION OF RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT
(18 U.S.C. § 1962(c))—CONDUCT OF OR PARTICIPATION IN THE AFFAIRS OF AN
ENTERPRISE THROUGH A PATTERN OF RACKETEERING ACTIVITY
(Against Defendants David Kent and Dufrin)**

160. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

161. David Kent and Dufrin conducted or participated in the affairs of the Oilpro Enterprise through their pattern of racketeering activity in violation of 18 U.S.C. § 1962(c). The Oilpro Enterprise is an enterprise whose activities affect interstate commerce.

162. David Kent and Dufrin were both employed by Oilpro during the period in question. David Kent and Dufrin conducted the affairs of the Oilpro Enterprise through the pattern of racketeering activity alleged herein. The specific affairs of the Oilpro Enterprise which David Kent, Dufrin, and Oilpro conducted were the unlawful appropriation of Plaintiffs’ proprietary information and trade secrets through the predicate acts alleged herein and the scheme to fraudulently induce DHI Group to purchase Oilpro.

163. As a result of David Kent and Dufrin conducting the affairs of the Oilpro Enterprise through a pattern of racketeering activity, Plaintiffs were thereby damaged in their business and property.

164. Plaintiffs request that this Court enter judgment that David Kent and Dufrin have violated 18 U.S.C. § 1962(c). Plaintiffs are entitled to damages incurred as a result of David Kent and Dufrin’s prohibited conduct, trebled by statute, plus reasonable attorneys’ fees and costs of suit.

**COUNT VII – VIOLATION OF RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT
(18 U.S.C. § 1962(d))—CONSPIRACY TO VIOLATE RICO §§ 1962(A), (B), AND (C)
(Against Defendants David Kent and Dufrin)**

165. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

166. David Kent and Dufrin conspired, in violation of 18 U.S.C. § 1962(d), to invest in, operate, grow, market, and sell Oilpro through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(a), to control the Oilpro Enterprise through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(b), and/or to conduct or participate in the affairs of the Oilpro Enterprise through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c).

167. David Kent and Dufrin knowingly agreed to commit predicate acts of racketeering, namely, multiple acts of wire fraud. The acts of wire fraud committed by the Defendants and the communications with DHI Group regarding the valuation and sale of Oilpro are evidence of this conspiratorial agreement, and they are also overt acts done by David Kent and Dufrin in furtherance of their conspiracy to grow, market, and sell the Oilpro enterprise through a pattern of racketeering activity and to conduct or participate in the affairs of Oilpro through a pattern of racketeering activity.

168. As a result of those overt acts in furtherance of these conspiracies that were also predicate acts of racketeering activity, Plaintiffs were injured in their business and property.

169. Plaintiffs request that this Court enter judgment that David Kent and Dufrin have violated 18 U.S.C. § 1962(d). Plaintiffs are entitled to damages incurred as a result of David Kent and Dufrin's prohibited conduct, trebled by statute, plus reasonable attorneys' fees and costs of suit.

**COUNT VIII— VIOLATION OF TEXAS UNIFORM TRADE SECRETS ACT (TEX. CIV. PRAC. & REM. CODE §§ 134A.001 ET. SEQ.)
(Against Defendants David Kent, Dufrin, and Oilpro)**

170. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

171. Plaintiffs' proprietary member information, internet search methods, and Google Analytics data constitute trade secrets within the meaning of the Texas Uniform Trade Secrets Act. This data is generally unknown information that Plaintiffs have taken reasonable efforts to

keep secret and has economic value to competitors such as Oilpro. It is not readily ascertainable by proper means.

172. David Kent, Dufrin, and Oilpro misappropriated Plaintiffs' trade secrets by acquiring their proprietary member information with knowledge that the information was acquired by improper means and being accessed and used without consent. Specifically, without Plaintiffs' consent, on numerous occasions, David Kent, Dufrin, and Oilpro knowingly and unlawfully appropriated Plaintiffs' member information.

173. David Kent, Dufrin, and Oilpro also misappropriated Plaintiffs' trade secrets by disclosure or use of Plaintiffs' member information without express or implied consent after using improper means to acquire knowledge of the information. Specifically, without Plaintiffs' consent, on numerous occasions, David Kent, Dufrin, and Oilpro knowingly and unlawfully appropriated Plaintiffs' member information and then used that information on numerous occasions to solicit Rigzone members to join Oilpro.

174. Dufrin and Oilpro misappropriated Plaintiffs' trade secrets by acquiring Plaintiffs' proprietary Google Analytics data with knowledge that the information was acquired by improper means and being accessed and used without consent. Specifically, without consent, on or about January 20, 2015 and June 10, 2015, Dufrin and Oilpro knowingly and unlawfully appropriated Plaintiffs' proprietary Google Analytics data.

175. Dufrin and Oilpro also misappropriated Plaintiffs' trade secrets by disclosure or use of this Google Analytics data without express or implied consent after using improper means to acquire knowledge of the data. Specifically, without consent, on or about January 20, 2015 and June 10, 2015, Dufrin and Oilpro used Plaintiffs' proprietary Google Analytics data and disclosed the data to David Kent.

176. David Kent, Dufrin, and Oilpro's acts constitute willful and malicious misappropriation.

177. As a result of the misappropriation of Plaintiffs' trade secrets by David Kent, Dufrin, and Oilpro, Plaintiffs suffered injury.

178. Pursuant to TEX. CIV. PRAC. & REM. CODE § 134A.004(a), Plaintiffs are entitled to recover damages for their actual loss caused by Defendants' misappropriation as described above, the unjust enrichment caused by Defendants' misappropriation that is not taken into account in computing actual loss, and additional damages as may be awarded by the trier of fact.

179. Pursuant to TEX. CIV. PRAC. & REM. CODE § 134A.004(b), Plaintiffs are also entitled to exemplary damages in an amount not exceeding twice any award made under § 134A.004(a) for Defendants' willful and malicious misappropriation as described above.

180. Pursuant to TEX. CIV. PRAC. & REM. CODE § 134A.005(b), Plaintiffs are also entitled to recover their court costs and reasonable and necessary attorneys' fees for Defendants' willful and malicious misappropriation as described above.

**COUNT IX – MISAPPROPRIATION OF CONFIDENTIAL INFORMATION (COMMON LAW)
(Against Defendants David Kent, Dufrin, and Oilpro)**

181. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

182. Plaintiffs' proprietary member information, internet search methods, and Google Analytics data constitute confidential information. This data is generally unknown information that Plaintiffs have taken reasonable efforts to keep secret and has economic value to competitors such as Oilpro. It is not readily ascertainable by proper means.

183. Plaintiffs have undertaken reasonable steps to protect its confidential information from disclosure and misuse, and Plaintiffs have obtained a competitive advantage from it.

184. Without permission, David Kent, Dufrin, and Oilpro unlawfully accessed and transferred Plaintiffs' confidential information by acquiring information from Rigzone's proprietary Members Database for their own advantage and to the detriment of Plaintiffs. Specifically, without consent, and on numerous occasions, David Kent, Dufrin, and Oilpro knowingly accessed Rigzone's Members Database and transferred Plaintiffs' confidential member information.

185. David Kent, Dufrin, and Oilpro also used Plaintiffs' member information, without consent, for their own advantage and to the detriment of Plaintiffs. Specifically, without consent, on numerous occasions, David Kent and Oilpro accessed and transferred Plaintiffs' confidential information and then repeatedly used that information to solicit Rigzone members to join Oilpro.

186. Dufrin and Oilpro unlawfully accessed and transferred Plaintiffs' confidential information by acquiring Plaintiffs' Google Analytics data for their own advantage and to the detriment of Plaintiffs. Specifically, without consent, on or about January 20, 2015 and June 10, 2015, Dufrin and Oilpro knowingly and unlawfully appropriated Plaintiffs' proprietary Google Analytics data.

187. Dufrin and Oilpro also used Plaintiffs' confidential Google Analytics data, without consent, for their own advantage and to the detriment of Plaintiffs. Specifically, without consent, on or about January 20, 2015 and June 10, 2015, Dufrin and Oilpro used Plaintiffs' proprietary Google Analytics data and disclosed the data to David Kent.

188. David Kent, Dufrin, and Oilpro intentionally acquired the confidential information through what Defendants knew was improper and unlawful means.

189. As a result of Defendants' misappropriation of Plaintiffs' confidential information, Plaintiffs suffered injury.

190. As a direct and proximate result of these wrongful acts, Defendants have caused Plaintiffs to suffer damages, including loss of goodwill, loss of trade secrets and confidential information, and the expense of investigating, reporting, and mitigating the breach of such confidential information, all in an amount in excess of the minimum jurisdictional limits of this Court. Defendants' wrongful actions have also caused, and will continue to cause, Plaintiffs irreparable harm and injury, including loss of goodwill, and loss of trade secrets and confidential information.

**COUNT X – VIOLATION OF THE TEXAS HARMFUL ACCESS BY COMPUTER ACT
(Against Defendants David Kent, Dufrin, and Oilpro)**

191. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

192. This cause of action is brought by Plaintiffs against David Kent, Dufrin, and Oilpro pursuant to the Texas Harmful Access by Computer Act, TEX. CIV. PRAC. & REM. CODE §§ 143.001 *et seq.*

193. On numerous occasions, including but not limited to during the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, and the Second Round of Hacks, David Kent, Dufrin, and Oilpro knowingly and intentionally accessed a computer, computer network, or computer system without the effective consent of the owners, the Plaintiffs, in violation of section 33.02 of the Texas Penal Code.

194. Plaintiffs have been injured by David Kent, Dufrin, and Oilpro's knowing and intentional access to Plaintiffs' computers, computer networks, and computer systems without consent, as Plaintiffs have had to incur significant costs in (a) assessing the potential damage to Plaintiffs' that have been caused by the Defendants' unauthorized access, use, and misappropriation, (b) responding to the loss of trade secrets and confidential information caused by Defendants'

actions, and (c) mitigating the loss of goodwill among Rigzone's members that has resulted from Defendants' unauthorized use, access and misappropriation. Plaintiffs have also been injured by the reduction in Rigzone's competitive advantages and the effect of Defendants' unauthorized access on Plaintiffs' ability to compete effectively in the marketplace.

195. Pursuant to TEX. CIV. PRAC. & REM. CODE § 143.002(a), Plaintiffs are entitled to recover their actual damages for injuries caused by David Kent, Dufrin, and Oilpro's knowing and intentional access to Plaintiffs' computer, computer network, or computer system without consent.

196. Pursuant to TEX. CIV. PRAC. & REM. CODE § 143.002(b), Plaintiffs are also entitled to recover their reasonable attorneys' fees and costs for bringing this clause of action.

**COUNT XI – VIOLATION OF THE TEXAS THEFT LIABILITY ACT (TEX. CIV. PRAC. & REM.
CODE §§ 134.001 ET. SEQ.)
(Against Defendants David Kent, Dufrin, and Oilpro)**

197. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

198. This cause of action is brought by Plaintiffs against David Kent, Dufrin, and Oilpro pursuant to the Texas Theft Liability Act, TEX. CIV. PRAC. & REM. CODE §§ 134.001 *et seq.*

199. Plaintiffs own and hold certain confidential and proprietary information and property, as described above. Plaintiffs have taken extensive measures to prevent from this confidential information from becoming available to persons other than those selected by Plaintiffs to access and to use its computer system for specified purposes.

200. Without consent, on numerous occasions, including but not limited to during the First Round of Hacks, the Google Analytics Hacks, Operation Resume Hoard, and the Second Round of Hacks, David Kent, Dufrin, and Oilpro knowingly and unlawfully appropriated Plaintiffs'

property with the intent to deprive Plaintiffs of their exclusive use of their member information and their Google Analytics data in violation of section 31.03(a) of the Texas Penal Code.

201. Defendants' unlawful appropriation of Plaintiffs' property constitutes theft, and Plaintiffs have suffered damages as a result of such theft.

202. Pursuant to TEX. CIV. PRAC. & REM. CODE § 134.005(a)(1), Plaintiffs are entitled to recover their actual damages resulting from Defendants' theft as described above and additional damages as may be awarded by the trier of fact.

203. Pursuant to TEX. CIV. PRAC. & REM. CODE § 134.005(b), Plaintiffs are also entitled to recover their court costs and reasonable and necessary attorneys' fees.

COUNT XII – CONVERSION
(Against Defendants David Kent, Dufrin, and Oilpro)

204. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

205. Through their conduct, David Kent, Dufrin, and Oilpro acquired, used, and controlled Plaintiffs' assets for their own benefit, constituting conversion.

206. David Kent, Dufrin, and Oilpro unlawfully appropriated Plaintiffs' proprietary Members Database and Google Analytics search processes, which constituted proprietary trade secrets and assets of Plaintiffs. David Kent, Dufrin, and Oilpro then exercised dominion and control over this information in a manner that was inconsistent with Plaintiffs' rights by incorporating it into Oilpro's business. As a result of David Kent, Dufrin, and Oilpro's conduct, Plaintiffs have been damaged.

207. The conduct above was deliberate and intentional, or in the alternative, grossly negligent and in reckless disregard for the rights of Plaintiffs, giving rise to liability for exemplary damages.

COUNT XIII – TRESPASS TO CHATTELS
(Against Defendants David Kent, Dufrin, and Oilpro)

208. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

209. Through their conduct, David Kent, Dufrin, and Oilpro interfered with Plaintiffs’ possession of their property and/or injured Plaintiffs’ property when David Kent, Dufrin, and Oilpro unlawfully misappropriated, used, and intentionally exercised wrongful control over Plaintiffs’ assets for their own benefit, constituting trespass to chattels.

210. David Kent, Dufrin, and Oilpro’s appropriation of Plaintiffs’ proprietary Members Database and Google Analytics search processes was not authorized.

211. As a result of David Kent, Dufrin, and Oilpro’s unauthorized interference with Plaintiffs’ property, Plaintiffs have been damaged.

COUNT XIV – FRAUD
(Against Defendant David Kent)

212. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

213. As the truth (or at least a significant part of it) has now been uncovered, it has become apparent that David Kent has for years been plotting to defraud Plaintiffs via a series of interrelated acts. The purpose of this fraud included to deprive DHI Group of the value of the Rigzone business that it bought from David Kent and others for over \$51 million and to deprive Rigzone of its trade secrets, proprietary data, and market advantages so that David Kent could build a competitor to sell either to DHI Group or another purchaser.

214. The seeds for this fraud began to be secretly planted years before. First, David Kent created the secret “backdoor” into Rigzone’s computer systems. a secret “backdoor” that has proven to be extremely difficult for even experts in the forensic technology field to discover and

decipher. Second, after creating this “backdoor”, David Kent kept it secret from Rigzone and DHI Group for years. Third, David Kent requested (unsuccessfully at first) that another Rigzone employee create a backup of the Rigzone website and place it on an external drive which mysteriously went missing near the time of David Kent's departure. Fourth, David Kent, Dufrin, and others repeatedly hacked into Plaintiffs' computer servers and stole member data and other proprietary information in order to compete with Plaintiffs and ultimately to attempt to sell for tens of millions of dollars (such as the hacked data created by Rigzone at considerable expense and effort). David Kent knew that as with any professional networking site the number of members was a significant driver behind Rigzone's value and the price that DHI Group paid for it. These are only a few examples of the deceptions and omissions that David Kent engaged in with respect to Rigzone and DHI Group over the years.

215. Taken together, David Kent's misrepresentations and omissions have had the effect of depriving Rigzone of the exclusive control over and access to its Members Database and of depriving DHI Group of the value that it sought to achieve when it paid David Kent and others \$51 million for Rigzone. Plaintiffs relied on David Kent in all of these circumstances to their detriment and have suffered actual damages as a result. Plaintiffs are also entitled to an award of exemplary damages against David Kent for his fraud.

**COUNT XV – BREACH OF FIDUCIARY DUTIES
(Against Defendant David Kent)**

216. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

217. At all times prior to his departure in September 2011, David Kent was a founder, officer, employee, and agent of Rigzone.

218. As such, David Kent owed Rigzone a duty of loyalty, which required him to act with candor, unselfishness, and good faith regarding Rigzone's affairs.

219. David Kent intentionally and willfully breached his duty of loyalty and fiduciary duty by failing to act with candor, unselfishness, and good faith regarding Rigzone's affairs by keeping his "backdoor" secret and intentionally and illegally acquiring confidential and proprietary information for use in his new enterprise, Oilpro.

220. As an employee, David Kent also owed Rigzone a fiduciary duty to maintain in confidence all confidential and proprietary trade secret information.

221. As a former employee and officer of Rigzone, David Kent continues to have and to owe a fiduciary duty to Rigzone to refrain from using Plaintiffs' confidential information or to commit any other disloyal act to Plaintiffs' actual or potential commercial disadvantage.

222. David Kent has willfully and intentionally breached and continues to breach his fiduciary responsibility to Rigzone through the acts set forth above.

223. David Kent intentionally and willfully violated his fiduciary duties to Rigzone by stealing Plaintiffs' data and member information to serve the interests of himself and the company he formed to compete with Rigzone.

224. As a direct and proximate result of David Kent's acts and omissions, Rigzone has suffered substantial damages, and David Kent, Oilpro, and other defendants have unlawfully profited.

225. David Kent's breaches of the duty of loyalty and fiduciary duty have caused, and unless enjoined will continue to cause, Plaintiffs serious and irreparable harm for which there exists no adequate remedy at law.

226. It is well settled under Texas law that courts may impose the equitable remedy of constructive trust upon a party who receives property or is otherwise unjustly enriched based on a breach of his fiduciary duty. Such a remedy is appropriate in this situation because Defendants obtained profits and revenues from members unlawfully obtained through the appropriation of Plaintiffs' trade secrets and proprietary information solely because of David Kent's breach of fiduciary duty. Because the benefits were obtained as a result of David Kent's breach of fiduciary duty, such benefits should, in equity, be transferred from Defendants to Plaintiffs by means of a constructive trust.

COUNT XVI - UNFAIR COMPETITION
(Against Defendants David Kent, Dufrin, and Oilpro)

227. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

228. Through the conduct of David Kent and Dufrin, Defendants unlawfully accessed and transferred Plaintiffs' confidential information by acquiring Plaintiffs' proprietary member information for their own advantage and to the detriment of Plaintiffs. This conduct constitutes unfair competition under Texas common law.

229. By unlawfully hacking into Plaintiffs' computer systems and misappropriating trade secrets and proprietary information, Defendants increased Oilpro's member base, profits and revenues, solicited and diverted Rigzone members, and implemented Rigzone's proprietary information into its own business, undermining many of Rigzone's competitive advantages in the marketplace.

230. Plaintiffs' proprietary Members Database and marketing strategies were created and developed through extensive time, labor, skill, and expense. Oilpro's use of this information in

competition with Rigzone gave (and continues to provide) Oilpro a special advantage in that competition.

231. By competing against Rigzone using the proprietary information that Oilpro unlawfully misappropriated, Oilpro engaged in unfair competition against Rigzone, Rigzone has suffered substantial damages, and Defendants unlawfully profited.

232. In addition, the tortious acts of David Kent, Dufrin, and Oilpro were willful and malicious. Consequently, Rigzone is entitled to an award of exemplary damages sufficient to punish them and to serve as a deterrent to such conduct.

233. David Kent, Dufrin, and Oilpro's conduct has caused and is causing irreparable injury to Rigzone and, unless enjoined by this Court, will continue to do so.

**COUNT XVII - TORTIOUS INTERFERENCE WITH PRESENT
AND PROSPECTIVE BUSINESS RELATIONSHIPS
(Against Defendants David Kent, Dufrin, and Oilpro)**

234. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

235. Rigzone had valid business and contractual relationships with hundreds of thousands of members, clients, and potential clients, using Rigzone's job placement services.

236. In the manner described herein, David Kent, Dufrin, and Oilpro intentionally, improperly and without privilege or justification interfered with the present and prospective business relations, contracts and rights between Rigzone and its members.

237. David Kent, Dufrin, and Oilpro, as described above, employed wrongful means in interfering with Rigzone's present and prospective business relationships with its members, customers, and recruiters.

238. David Kent, Dufrin, and Oilpro unlawfully secured Plaintiffs' confidential member information and confidential search engine analytics, both of which constituted proprietary trade secrets and assets of Plaintiffs. David Kent, Dufrin, and Oilpro then exercised dominion and control over this information in order to divert existing Rigzone members and actual and potential job placement transactions away from Rigzone and into Oilpro's business.

239. David Kent, Dufrin, and Oilpro's interference with Rigzone's present and prospective contractual relations was and continues to be intentional, malicious, willful, wanton and outrageous, entitling Rigzone to exemplary damages against David Kent, Dufrin, and Oilpro, and any other persons acting in concert with them that are identified in discovery.

240. As a direct and proximate result of David Kent, Dufrin, and Oilpro's acts, omissions, and unfair competition, Rigzone has suffered substantial damages and David Kent, Dufrin, and Oilpro have unlawfully profited.

241. Furthermore, David Kent, Dufrin, and Oilpro's conduct has caused and is causing irreparable injury to Rigzone and, unless enjoined by this Court, will continue to do so.

**COUNT XVIII – CIVIL CONSPIRACY
(Against All Defendants)**

242. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

243. Defendants and others, known and unknown, willfully and knowingly, did combine, conspire, confederate, and agree together and with each other to commit offenses against the laws of the United States and Texas, to wit, violations of Title 18, United States Code, Sections 1030 (a)(2)(C), 1030(a)(4), 1030(a)(5)(A), 1030 (g); Title 18, United States Code, Sections 2701(a)(1), 2707; Title 18, United States Code, Section 1343; the Texas Uniform Trade Secrets Act; the Texas Harmful Access by Computer Act; the Texas Theft Liability Act.

244. In addition, Defendants conspired to unlawfully appropriate Plaintiffs' trade secrets and proprietary information in order to, *inter alia*, expand Oilpro's business, inflate the value of Oilpro, and commit fraud against Plaintiffs.

245. As members of this unlawful conspiracy, Defendants had a meeting of the minds as to the object of their conspiracy. In particular, Defendants agreed and understood that the object of their goal was to commit the wrongful acts detailed above.

246. Each Defendant has committed unlawful and overt acts in furtherance of the conspiracy including, but not limited to, participating, supporting, approving or otherwise acquiescing in the wrongful conduct described above.

247. Based on this unlawful conspiracy, Plaintiffs have been damaged. Accordingly, Plaintiffs seek to recover actual, compensatory, and consequential damages.

248. Further, because the acts pursuant to the conspiracy were committed knowingly, willfully, maliciously, fraudulently, and with gross negligence, Plaintiffs seek to recover exemplary damages.

249. The aforementioned conduct of Defendants was committed with an evil mind, with the intent of depriving Plaintiffs of their property and/or legal rights or otherwise causing injury, and was malicious and despicable conduct that subjected Plaintiffs to an unjust injury in conscious disregard of the Plaintiffs' rights so as to justify an award of exemplary damages.

**COUNT XIX— AIDING AND ABETTING
(Against All Defendants)**

250. Plaintiffs repeat and reallege the allegations set forth in paragraphs 1–117 as if fully set forth herein.

251. By their conduct set forth above, Defendants aided and abetted David Kent and Dufrin in their commission of wire fraud, conspiracy to commit wire fraud, and the other criminal violations asserted in this Complaint.

252. Defendants, directly or indirectly, with intent to deceive or defraud, or with reckless disregard for the truth or the law, materially aided David Kent's and Dufrin's violations of Title 18, United States Code, Sections 1030 (a)(2)(C), 1030(a)(4), 1030(a)(5)(A), 1030 (g); Title 18, United States Code, Sections 2701(a)(1), 2707; Title 18, United States Code, Section 1343; the Texas Uniform Trade Secrets Act; the Texas Harmful Access by Computer Act; the Texas Theft Liability Act; and common law causes of action as set forth above in Counts I–IV, VII–XIII, and XVI–XVII, and, therefore, are jointly and severally liable to the same extent as if they were primarily liable.

253. Further, Defendants knew that David Kent and Dufrin were unlawfully appropriating Plaintiffs' personal property, intended to assist David Kent and Dufrin in doing so, and did assist David Kent and Dufrin by accessing, downloading, possessing, and using the misappropriated information.

254. Defendants' assistance was a substantial factor in causing these unlawful acts to be performed and in furthering Defendants' scheme to unlawfully access and misappropriate Plaintiffs' trade secrets and proprietary information.

VI. Application for Preliminary Injunctive Relief and Permanent Injunctive Relief

255. Plaintiffs incorporate each of the foregoing paragraphs above as if fully set forth herein.

256. Plaintiffs have already suffered and will likely suffer further irreparable injury from Defendants' illegal acquisition, use, and maintenance of the data, information, documents, and other property obtained from Plaintiffs. Plaintiffs have already suffered and are likely to continue to suffer damage to goodwill and reputation with Rigzone's members as long as

Defendants are in a position to use or disclose the confidential information and documents pertaining to Rigzone's members and Rigzone's business. In addition, Plaintiffs' ability to compete effectively in the marketplace will continue to be compromised as long as Defendants continue to possess confidential information and documents regarding Rigzone's members and website analytics.

257. While Plaintiffs are seeking an award for, *inter alia*, their legal damages and to recoup the wrongful gains obtained by Defendants, there is no adequate remedy at law to fully rectify the actual and prospective loss to Plaintiffs as a result of Defendants' continued misappropriation of their confidential information and documents. The recovery of monetary damages alone cannot prevent the further use or disclosure of the confidential information which Defendants have misappropriated.

258. There is a substantial likelihood that Plaintiffs will prevail on the merits of this case. Defendants' misappropriation of such information is a clear violation of their legal obligations for which no reasonable defense can be offered.

259. Plaintiffs therefore request a preliminary and permanent injunction pursuant to Federal Rule of Civil Procedure 65 against Defendants, requiring that Defendants:

- a. Provide a copy of all materials, data, and information obtained from Rigzone and/or DHI Group and/or Google's computer systems and all information and data obtained by using the misappropriated data, including all information and data obtained through "network effects" and/or the social networks of members whose information was misappropriated, to the Court and Plaintiffs' counsel;
- b. Delete all materials, data, and information obtained from Rigzone and/or DHI Group and/or Google's computer systems and all information and data obtained by using the misappropriated data, including all information and data obtained through "network effects" and/or the social networks of members whose information was misappropriated;

- c. Make no further use or disclosure whatsoever of any and all of Plaintiffs' trade secrets and other confidential information;
- d. Identify all persons to whom Plaintiffs' trade secrets and other confidential information have been disclosed;
- e. Refrain from using any of Plaintiffs' trade secrets or confidential information and from conducting, soliciting, or performing any business, service, member, customer, or potential member or customer based thereon, regardless of whether such business, service, member, or customer opportunity becomes available after the deletion of the misappropriated data;
- f. Refrain from contacting Rigzone's current and former employees;
- g. Refrain from soliciting or conducting business with any Rigzone member or customer whose information was included in the misappropriated data;
- h. Refrain from conducting business with any party who was a Rigzone member or prospective member before January 1, 2016;
- i. Remove all Oilpro members whose information was included in the misappropriated data from Oilpro's website and other job placement services or who became Oilpro members through the use of misappropriated data, including all Oilpro members obtained through "network effects" and/or social networks of members whose information was misappropriated.

260. Defendants would face no significant harm by complying with an injunction barring their continued possession, use, or disclosure of the confidential information because the contents of such material do not belong to them. In contrast, in the absence of such an injunction, the damage to Plaintiffs which could result from Defendants' continued possession, use, or disclosure of these materials cannot be undone.

261. The public interest favors issuance of the requested injunctive relief and will be served by the promotion of ethical behavior and the protection of property rights and confidential member information. In addition, such protection is critical to persons whose private information is contained in such materials, including, but not limited to, the Plaintiffs' members.

262. Plaintiffs are willing to post a bond in the amount, if any, that the court deems appropriate.

263. Plaintiffs ask the court to set their application for preliminary injunction for hearing and, after hearing the request, to issue a preliminary injunction against Defendants.

264. Plaintiffs ask the court to include the application for permanent injunctive relief in a full trial on the merits of this case and, after the trial, to issue a permanent injunction against Defendants, as well as to provide Plaintiffs with the other relief it has requested.

VII. Attorneys' Fees

265. Plaintiffs have employed the undersigned attorneys to prosecute this suit on their behalf. Plaintiffs are entitled to recover reasonable and necessary attorneys' fees and costs incurred in the prosecution of this lawsuit pursuant to, *inter alia*, 18 U.S.C. § 2707(c), 18 U.S.C. §§ 1961 *et seq.*, and TEX. CIV. PRAC. & REM. CODE § 134A.005(b), § 134.005(b), and § 143.002(b).

VIII. Jury Demand

266. Having paid the required fee, Plaintiffs demand a trial by jury upon all issues raised in this Complaint.

IX. Prayer

267. For the foregoing reasons, Plaintiffs respectfully request that, following a jury trial, it be granted the following relief:

- a) judgment in favor of Plaintiffs and against Defendants on Counts I through XIX;
- b) award of compensatory damages, disgorgement of revenues and/or gains wrongfully acquired, treble damages, and exemplary damages;
- c) entry of a preliminary injunction, thereafter to be made permanent, that, among other things, enjoins Defendants from keeping, using, or disclosing any information, documents or other property owned

by or obtained from Plaintiffs or any of Rigzone's members, and granting all other injunctive relief requested herein;

- d) entry of an order directing Defendants to return all copies of Plaintiffs' information or documents obtained from their unauthorized access to Plaintiffs' computer systems;
- e) entry of an order directing Defendants to identify any person or persons to whom any information or documents obtained from their unauthorized access to Plaintiffs' computer systems has been disclosed;
- f) award of reasonable attorneys' fees and the costs of prosecuting this action;
- g) award of pre- and post-judgment interest on damages as allowed by law; and
- h) an award to Plaintiffs of all other relief, in law and in equity, to which it may show itself to be entitled or as the Court deems just and appropriate.

DATED: June 10, 2016

Respectfully submitted,

BAKER BOTTS L.L.P.

By: /s/ Kevin T. Jacobs

Kevin T. Jacobs
State Bar No. 24012893
Federal ID No. 26665
Justin Lipe
State Bar No. 24083401
Federal ID No. 2053646
Christine Ng
State Bar No. 24087678
Federal ID No. 2210307
One Shell Plaza
910 Louisiana Street
Houston, Texas 77002-4995
Telephone: (713) 229-1234
Facsimile: (713) 229-7847
kevin.jacobs@bakerbotts.com
justin.lipe@bakerbotts.com
christine.ng@bakerbotts.com

ATTORNEYS FOR PLAINTIFFS
DHI GROUP, INC. f/k/a DICE
HOLDINGS, INC. AND
RIGZONE.COM, INC.

OF COUNSEL:
Richard B. Harper
Douglas W. Henkin
BAKER BOTTS L.L.P.
30 Rockefeller Plaza
New York, NY 10112
Telephone: (212) 408-2500
Facsimile: (212) 408-2501
richard.harper@bakerbotts.com
douglas.henkin@bakerbotts.com